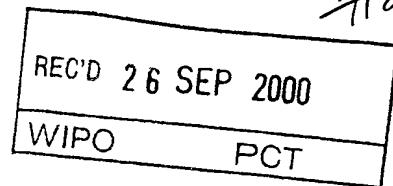




10/048216



BREVET D'INVENTION

FR 00/02024

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

DOCUMENT DE PRIORITÉ

COPIE OFFICIELLE

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a OU b)

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 04 SEP. 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

BEST AVAILABLE COPY

Martine PLANCHE

SIEGE
INSTITUT
NATIONAL DE
LA PROPRIETE
INDUSTRIELLE

26 bis, rue de Saint Petersbourg
75800 PARIS Cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

This Page Blank (uspto)



INSTITUT
NATIONAL DE
LA PROPRIÉTÉ
INDUSTRIELLE

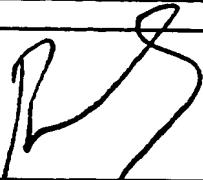
BREVET D'INVENTION

26bis, rue de Saint-Pétersbourg
75800 Paris Cedex 08
Téléphone: 01 53.04.53.04 Télécopie: 01.42.94.86.54

Code de la propriété intellectuelle-livreVI

REQUÊTE EN DÉLIVRANCE

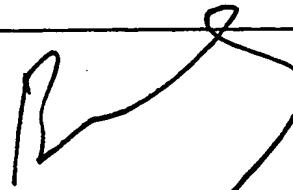
0	RESERVE A L'INPI			
0-1	Date de remise des pièces	30.07.99		
0-2	N° d'enregistrement national	9310106		
0-3	Département de dépôt	99		
0-4	Date de dépôt	30.07.99		
0-6	Titre de l'invention	Schémas de signature à base de logarithme discret avec reconstitution partielle ou totale du message		
0-8	Etablissement du Rapport de Recherche	immédiat		
0-9	Votre référence dossier	GEM765		
1	DEMANDEUR(s)			
1-1	Norm Suivi par: Adresse rue Adresse code postal et ville Pays Nationalité Forme juridique N° SIREN Code APE-NAF N° de téléphone N° de télécopie Courrier électronique	GEMPLUS Pierre BRUYERE Avenue du Pic de Bretagne Parc d'activités de Gèmenos 13881, GEMENOS France France S.C.A 349 711 200 321B 04.42.36.69.06. 04.42.36.63.43. nathalie.herau@gemplus.com		
4	Déclaration de PRIORITE ou REQUETE du bénéfice de la date de dépôt d'une demande antérieure	Etat	Date	N° de la demande
6	Documents et Fichiers joints	Fichier électronique	Pages	Détails
6-1	Description	easy765.doc	25	
6-2	Revendications	easy765.doc	23	24
6-3	Abrégé	easy765.doc	1	
6-4	Listage de séquences			
6-5	Rapport de recherche			
7	Mode de paiement	Prélèvement du compte courant		
7-1	Numéro du compte client	2381		
7-2	Remboursement à effectuer sur le compte n°	2381		
8	REDEVANCES	Devise	Taux	Montant à payer
	062 Dépôt	FRF	250.00	250.00
	063 Rapport de recherche (R.R.)	FRF	4 200.00	4 200.00
	068 Revendication à partir de la 11ème	FRF	115.00	1 610.00
	Total à acquitter	FRF		6 060.00

10	Signature	
10-1	<i>Signé par</i>	<p>Bernard NONNENMACHER Directeur de la Propriété Industrielle GEMPLUS</p> 

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI."

BREVET D'INVENTION

Désignation de l'inventeur

Référence utilisateur:	GEM765
Référence système:	111111 729774,640653704
N° d'enregistrement national:	99-10-106
Titre de l'invention:	Schémas de signature à base de logarithme discréts avec reconstitution partielle ou totale du message
Le(s) soussigné(s):	Bernard NONNENMACHER Directeur de la Propriété Industrielle GEMPLUS
Désigne(nt) en tant qu'inventeur(s):	
Inventeur 1	Nom, Prénom: STERN, Jacques Adresse: 7 rue P. Nicole F-75005 PARIS France
Inventeur 2	Nom, Prénom: NACCACHE, David Adresse: 7 rue Chaptal F-75009 PARIS France
Inventeur 3	Nom, Prénom: CORON, Jean-Sébastien Adresse: 4 rue Léon de Lagrange F-75015 PARIS France
Signé par:	 Bernard NONNENMACHER Directeur de la Propriété Industrielle GEMPLUS
En qualité de:	Directeur de la Propriété Industrielle
Date:	29 juil. 1999

DOCUMENT COMPORTANT DES MODIFICATIONS

Un changement apporté à la rédaction des revendications d'origine, sauf si celui-ci découle des dispositions de l'article R.612-36 du code de la Propriété Intellectuelle, est signalé par la mention «R.M.» (revendications modifiées).

SCHEMAS DE SIGNATURE A BASE DE
LOGARITHME DISCRET AVEC RECONSTITUTION
PARTIELLE OU TOTALE DU MESSAGE

L'invention consiste en deux nouveaux schémas de
signature électronique basés sur le problème du
logarithme discret, le premier permettant la
reconstitution totale du message, le second
5 permettant la reconstitution partielle du
message, ainsi que deux techniques permettant de
réduire la taille des signatures électroniques.

Une signature électronique d'un message est un
10 nombre dépendant à la fois d'une clé secrète
connue seulement de la personne signant le
message, ainsi que du contenu du message à
signer. Une signature électronique doit être
vérifiable: il doit être possible pour une
15 tierce personne de vérifier la validité de la
signature, sans que la connaissance de la clé
secrète de la personne signant le message ne
soit requise.

20 Il existe 2 types de schéma de signature
électronique:

- Schémas de signature électronique nécessitant
le message original pour la vérification de la
25 signature.

- Schémas de signature électronique avec
reconstitution du message. Le message original

est obtenu d'après la signature elle-même. Le message original n'étant pas nécessaire pour vérifier la signature, la taille totale de la signature est plus courte.

5

Il existe de nombreux procédés de signature électronique. Les plus connus sont:

- Schéma de signature RSA: c'est le schéma de signature électronique le plus largement utilisé. Sa sécurité est basée sur la difficulté de la factorisation de grands nombres.

15 - Schéma de signature Rabin. Sa sécurité est aussi basée sur la difficulté de la factorisation de grands nombres.

20 - Schéma de signature de type El-Gamal. Sa sécurité est basée sur la difficulté du problème du logarithme discret. Le problème du logarithme discret consiste à déterminer, s'il existe, un entier x tel que $y=g^x$ avec y et g deux éléments d'un ensemble E possédant une structure de groupe.

25

- Schéma de signature Schnorr. Il s'agit d'une variante du schéma de signature de type El-Gamal.

30 - Il existe une autre variante du schéma de signature de type El-Gamal permettant la

reconstitution totale du message, appelée schéma de signature Nyberg et Rueppel. Ce schéma est décrit dans l'article « A new signature scheme based on the DSA, giving message recovery » paru 5 dans « Proceedings of the first ACM conference on communications and computer security, 1993, 58-61 ». Une variante de schéma à base de courbe elliptique est décrite dans le document « IEEE P1363 draft. Standard specifications for public 10 key cryptography. August 1998 ». Cette variante utilise une fonction de redondance R , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté O et un point G de la courbe, lequel point G est générateur d'un sous- 15 groupe d'ordre un nombre premier r . La clé privée est un entier positif s inférieur à r et la clé publique est le point $W=s.G$, la notation $s.G$ désignant la somme, au sens de l'addition de la courbe elliptique, de s points pris égaux à 20 G . Le procédé de génération de la signature d'un message m comporte les 5 étapes suivantes:

- 1) Générer un nombre aléatoire u compris entre 0 et $r-1$ et calculer $V=u.G$.
- 25 2) Calculer l'entier $f=R(m)$.
- 3) Associer au point V un entier i et calculer $c=i+f$ modulo r . Retourner à l'étape 1) si $c=0$
- 4) Calculer $d=u-s*c$ modulo r .
- 5) La signature est la paire d'entiers (c,d) .

Le procédé de vérification de la signature comporte les 4 étapes suivantes:

- 1) Si c n'appartient pas à l'intervalle $[1, r-1]$ ou si d n'appartient pas à l'intervalle $[0, r-1]$, la signature n'est pas valide.
- 2) Calculer le point $P = d.G + c.W$. Si $P = O$, la signature n'est pas valide.
- 3) Associer au point P l'entier i et calculer $f = c - i \text{ modulo } r$.
- 4) Retrouver le message m à partir de f et vérifier que $f = R(m)$. Si oui, la signature du message m est valide. Sinon, la signature n'est pas valide.

15

Le premier procédé de l'invention consiste en une autre variante d'un schéma de signature de type El-Gamal. Cette variante permet la reconstitution totale du message. La variante est décrite dans le cadre de l'utilisation de courbes elliptiques. Il est cependant possible d'utiliser cette variante dans tout ensemble possédant une structure de groupe pour lequel le problème du logarithme discret est difficile, par exemple le groupe multiplicatif des entiers modulo un nombre premier ou le sous-groupe multiplicatif d'ordre un grand nombre premier r des entiers modulo un nombre premier p avec r divisant $p-1$. Cette variante utilise une fonction de redondance R , une courbe elliptique formant une structure de groupe dont l'élément

zéro est noté O et un point G de la courbe, lequel point G est générateur d'un sous-groupe d'ordre un nombre premier r . La clé privée est un entier positif s inférieur à r et la clé 5 publique est le point $W=s.G$. Cette variante utilise une constante entière k non nulle. Le procédé de génération de la signature comporte les 4 étapes suivantes:

- 10 1) Générer un nombre aléatoire u compris entre 1 et $r-1$ et calculer $V=u.G$.
- 2) Associer au point V un entier i et calculer $c=i+f$ modulo r . Si $c=0$, retourner à l'étape 1).
- 3) Calculer l'entier $d=u^{-1}*(k+s*c)$ modulo r . Si 15 $d=0$, retourner à l'étape 1).
- 4) La signature est la paire d'entiers (c,d) .

Le procédé correspondant de vérification de la signature comporte les 6 étapes suivantes:

- 20 1) Si c n'appartient pas à l'intervalle $[1,r-1]$ ou si d n'appartient pas à l'intervalle $[1,r-1]$, la signature n'est pas valide.
- 2) Calculer les entiers $h= d^{-1}$ modulo r , $h_1=k*h$ modulo r et $h_2=c*h$ modulo r .
- 25 3) Calculer le point $P= h_1G+ h_2W$. Si $P=O$, la signature n'est pas valide.
- 4) Associer au point P un entier i .
- 5) Calculer l'entier $f=c-i$ modulo r .
- 30 6) Retrouver le message m à partir de f et vérifier que $f=R(m)$. Si oui, la signature du

message m est valide. Sinon, la signature n'est pas valide.

Le procédé précédemment décrit permet donc 5 d'obtenir un schéma de signature électronique dont la sécurité est basée sur la difficulté du problème du logarithme discret et permettant la reconstitution totale du message.

-----10-----L'invention comprend également un-----
second procédé de signature
électronique permettant la
reconstitution partielle du message. Le
schéma de signature décrit précédemment
15 permet la reconstitution totale du
message. Cependant, la taille totale du
message à signer est limitée par la
taille des arguments de la fonction de
redondance R . Le second procédé de
l'invention permet de signer un message
20 d'une taille quelconque. Le message m à
signer est divisé en 2 parties: la
première partie m_1 de taille constante
est reconstituée à partir de la
signature, la deuxième partie m_2 est
25 transmise avec la signature du message.
La taille totale de la signature et du
message à transmettre est donc diminuée
de la taille de la partie m_1 . Le schéma
de signature est décrit dans le cadre
30 de l'utilisation de courbes-----

elliptiques. Il est cependant possible d'utiliser ce schéma dans tout ensemble possédant une structure de groupe pour lequel le problème du logarithme discret est difficile, par exemple le groupe multiplicatif des entiers modulo un nombre premier ou le sous-groupe multiplicatif d'ordre un grand nombre premier r des entiers modulo un nombre premier p avec r divisant $p-1$. Le schéma de signature utilise une fonction de redondance R , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté 0 et un point G de la courbe, lequel point G est générateur d'un sous-groupe d'ordre un nombre premier r . La clé privée est un entier positif s inférieur à r et la clé publique est le point $W=s.G$. Le procédé de génération de la signature d'un message m constitué des messages m_1 et m_2 comporte les 6 étapes suivantes:

- ```

25 1) Générer un entier aléatoire u compris entre 1
 et r-1 et calculer V=u.G
2) Calculer $f_1=R(m_1)$
3) Associer au point V un entier i et calculer
 $c=i + f_1$ modulo r. Si $c=0$, retourner à l'étape 1.
30 4) Calculer $f_2=H(m_2)$, où H est une fonction de
 hachage.

```

5) Calculer l'entier  $d = u^{-1} * (f_2 + s * c)$  modulo  $r$ . Si  $d = 0$ , retourner à l'étape 1.

6) La signature est le couple d'entiers  $(c, d)$

5 Le procédé de vérification de la signature prend  
en entrée une paire d'entiers  $(c, d)$  et le  
message partiel  $m_2$  et comprend les 7 étapes  
suivantes:

10 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.

2) Calculer  $f_2 = H(m_2)$ , où  $H$  est une fonction de hachage.

15 3) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  modulo  $r$  et  $h_2 = c * h$  modulo  $r$ .

4) Calculer le point  $P = h_1 G + h_2 W$ . Si  $P = O$ , la signature n'est pas valide.

5) Associer au point  $P$  l'entier  $i$ .

20 6) Calculer l'entier  $f_1 = c - i$  modulo  $r$ .

7) Obtenir le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1 = R(m_1)$ . Si oui, la signature du message  $m$  est valide. Sinon, la signature n'est pas valide.

25

Le procédé précédent décrit permet donc d'obtenir un schéma de signature électronique dont la sécurité est basée sur la difficulté du logarithme discret et permettant la reconstitution partielle du message. L'intérêt

30 d'un tel schéma est de diminuer la taille totale

de la signature et du message à transmettre sans toutefois imposer de contrainte de taille à ce message.

5 L'invention consiste également en 2 techniques générales permettant de minimiser la taille totale de la signature et du message à transmettre. La première technique consiste à inclure une partie du message à l'intérieur de 10 la signature en choisissant convenablement les données aléatoires utilisées lors de la génération de la signature. La deuxième technique consiste à supprimer une partie des octets représentant la signature, la 15 reconstitution complète de la signature s'effectuant durant la phase de vérification.

Le troisième procédé de l'invention consiste en une amélioration du schéma de signature de 20 Nyberg-Rueppel rappelé précédemment, et consiste à inclure une partie du message de taille  $t$  octets dans l'entier  $d$  défini précédemment,  $t$  étant un entier petit. Dans ce procédé, les  $t$  octets de poids faible de l'entier  $d$  contiennent 25  $t$  octets du message. Le troisième procédé de l'invention permet donc d'augmenter de  $t$  octets la taille du message à signer par rapport au schéma de signature de Nyberg-Rueppel décrit précédemment. Le troisième procédé utilise une 30 fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément

zéro est noté 0 et un point G de la courbe, lequel point G est générateur d'un sous-groupe d'ordre un nombre premier r. La clé privée est un entier positif s inférieur à r et la clé 5 publique est le point  $W=s.G$ . Le procédé de génération de la signature d'un message m comporte les 5 étapes suivantes:

- 1) Enlever les t octets de poids faible du 10 message  $m$  et mémoriser le résultat dans  $m'$ . Calculer  $f=R(m')$ .
- 2) Générer un nombre aléatoire u compris entre 1 et  $r-1$  et calculer  $V=u.G$ .
- 3) Associer au point V un entier i et calculer 15  $c=i+f$  modulo r. Retourner à l'étape 1) si  $c=0$ .
- 4) Calculer l'entier  $d=u-s*c$  modulo r. Si d n'est pas égal à m modulo  $2^{8t}$  retourner à l'étape 2).
- 5) La signature est le couple d'entiers  $(c, d)$ .

20

Le procédé de vérification de la signature comporte les 5 étapes suivantes:

- 1) Si c n'appartient pas à l'intervalle  $[1, r-1]$  25 ou si d n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide.
- 2) Calculer le point  $P=d.G+c.W$ . Si  $P=0$ , la signature n'est pas valide.
- 3) Associer au point P l'entier i.
- 30 4) Calculer l'entier  $f=c-i$  modulo r.

5) Obtenir le message  $m'$  à partir de  $f$  et vérifier que  $f=R(m')$ . Si ce n'est pas le cas, la signature n'est pas valide. Si c'est le cas, la signature est valide et le message  $m$  est la concaténation au message  $m'$  des  $t$  octets de poids faible de l'entier  $d$ .

---

Il est possible d'effectuer un prétraitement des données permettant d'accélérer la génération des signatures selon le schéma de signature décrit précédemment. Le procédé de prétraitement prend en entrée la clé secrète  $s$  et consiste à mettre en mémoire dans une table un grand nombre de valeurs  $(i, x_u)$  avec  $x_u=u-s*i$  modulo  $r$  et  $i$  étant l'entier associé au point  $V=u.G$ , de telle sorte que ces valeurs puissent être accédées par le reste de  $x_u$  modulo  $2^{8t}$ . Le procédé de génération de signature avec prétraitement des données utilise une fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ .

Le procédé de génération de signature avec prétraitement des données comporte les 8 étapes suivantes :

30 1) Enlever les  $t$  octets de poids faible du message  $m$  et mémoriser le résultat dans le

message  $m'$ . Calculer  $f=R(m')$ . Les  $t$  octets de poids faible du message  $m$  sont mémorisés dans l'entier  $\delta$ .

- 2) Calculer l'entier  $y=s*f$  modulo  $r$  et l'entier  $\lambda=y$  modulo  $2^{8t}$ .
- 3) Si  $y < r/2$ , exécuter d'abord l'étape 4 et ensuite l'étape 5, sinon exécuter d'abord l'étape 5 et ensuite l'étape 4.
- 4) Accéder aux éléments de la table dont le reste modulo  $2^{8t}$  est  $\lambda+\delta$  modulo  $2^{8t}$  et sélectionner un élément tel que  $x_u$  est supérieur ou égal à  $y$ . Si un tel élément existe, il est supprimé de la table et le procédé passe à l'étape 6)
- 5) Accéder aux éléments de la table, dont le reste modulo  $2^{8t}$  est  $\lambda+\delta+r$  modulo  $2^{8t}$  et sélectionner un élément tel que  $x_u$  est inférieur à  $y$ . Si un tel élément existe, il est supprimé de la table et le procédé passe à l'étape 6)
- 6) Calculer l'entier  $d = x_u - y$  modulo  $r$ .
- 7) Obtenir l'entier  $i$  associé à  $x_u$  et calculer  $c = i + f$  modulo  $r$ .
- 8) La signature est le couple d'entiers  $(c, d)$ .
- 25 Le quatrième procédé de l'invention consiste en une amélioration du schéma de signature à base de logarithme discret avec reconstitution partielle du message décrit précédemment. Le quatrième procédé de l'invention consiste à inclure une partie du message de taille  $t$  octets

dans l'entier  $d$  défini précédemment,  $t$  étant un entier petit. Dans ce procédé, les  $t$  octets de poids faible de l'entier  $d$  contiennent  $t$  octets du message. Le quatrième procédé de l'invention 5 permet donc de diminuer de  $t$  octets la taille totale de la signature et du message à transmettre. Le schéma de signature utilise une fonction de redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément 10 zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé 15 publique est le point  $W=s.G$ . Le procédé de génération de la signature d'un message  $m$  constitué des messages  $m_1$  et  $m_2$  comporte les 6 étapes suivantes:

- 1) Générer un entier aléatoire  $u$  compris entre 1 20 et  $r-1$  et calculer  $V=u.G$
- 2) Calculer  $f_1=R(m_1)$
- 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f_1$  modulo  $r$ . Si  $c=0$ , retourner à l'étape 1.
- 4) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de 25 hachage.
- 5) Calculer l'entier  $d=u^{-1}*(f_2+s*c)$  modulo  $r$ . Si  $d=0$  ou si  $d$  n'est pas égal à  $m_2$  modulo  $2^{8t}$  retourner à l'étape 1.
- 6) La signature est le couple d'entiers  $(c,d)$  et 30 le message à transmettre est  $m'_2$  consistant en  $m_2$  privé de ses  $t$  octets de poids faible.

Le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c, d)$  et le message partiel  $m'_2$ , et comprend les 8 étapes suivantes:

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.
- 10 2) Compléter  $m'_2$  en  $m_2$  en lui ajoutant les  $t$  octets de poids faible de  $d$ .
- 3) Calculer  $f_2 = H(m_2)$ , où  $H$  est une fonction de hachage.
- 4) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  modulo  $r$  et  $h_2 = c * h$  modulo  $r$ .
- 15 5) Calculer le point  $P = h_1 G + h_2 W$ . Si  $P = O$ , la signature n'est pas valide.
- 6) Associer au point  $P$  l'entier  $i$ .
- 7) Calculer l'entier  $f_1 = c - i$  modulo  $r$ .
- 20 8) Obtenir le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1 = R(m_1)$ . Si oui, la signature du message  $m$  est valide. Sinon, la signature n'est pas valide.
- 25 Le cinquième procédé de l'invention consiste à supprimer  $t$  octets de la chaîne d'octets représentant l'entier  $d$  lorsque la signature est le couple d'entiers  $(c, d)$ .
- 30 Ce procédé s'applique au schéma de signature de Nyberg et Rueppel ainsi qu'au schéma de signature avec reconstitution partielle du

message précédemment décrit. Le procédé modifié de génération de signature comporte les 2 étapes suivantes.

- 5 1) Générer la signature du message  $m$  en utilisant le schéma de signature de Nyberg et Rueppel ou le schéma de signature avec reconstitution partielle du message précédemment décrit, pour obtenir le couple d'entiers  $(c, d)$ .
- 10 2) Calculer  $d'$ , quotient entier de la division de l'entier  $d$  par  $2^{8t}$ . La signature est le couple d'entiers  $(c, d')$ .

Le procédé modifié de vérification de signature prend en entrée un couple  $(c, d')$  et un message  $m_2$  et comporte les 2 étapes suivantes dans le cas de l'utilisation du schéma de signature avec reconstitution partielle du message précédemment décrit :

- 20 1) Pour  $i$  allant de 0 à  $2^{8t}-1$ , calculer l'entier  $d=d'*2^{8t}+i$  et exécuter le procédé de vérification de signature avec reconstitution partielle du message précédemment décrit, la signature à vérifier étant  $(c, d)$ . Si le procédé de vérification de signature reconnaît la signature  $(c, d)$  comme valide, la signature est valide, et le procédé est terminé.
- 25 2) Si l'étape 1) n'a pas abouti, la signature n'est pas valide.

Dans le cas de l'utilisation du schéma de signature de Nyberg-Rueppel, le procédé de vérification de signature prend en entrée un couple  $(c, d')$  et comporte les 5 étapes suivantes

5 :

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.
- 2) Calculer le point  $P = d' * 2^{8t} \cdot G + c \cdot W$
- 3) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les étapes suivantes:
  - 3)a) Si  $P=O$ , exécuter l'étape 3)d)
  - 3)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f = c - i$  modulo  $r$ .
  - 3)c) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f = R(m)$ . Si oui, exécuter l'étape 5).
  - 3)d) Remplacer  $P$  par  $P+G$ .
- 4) La signature n'est pas valide et le procédé est terminé.
- 5) Si l'entier  $d = d' * 2^{8t} + j$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide, sinon la signature est valide et le procédé est terminé.

25

Le sixième procédé de l'invention consiste en une modification du schéma de signature de Nyberg et Rueppel permettant d'augmenter de  $t$  octets la taille des messages à signer,  $t$  étant une variable entière. Le sixième procédé utilise une fonction de redondance  $R$ , une courbe

elliptique formant une structure de groupe dont l'élément zéro est noté 0 et un point G de la courbe, lequel point G est générateur d'un sous-groupe d'ordre un nombre premier r. La clé 5 privée est un entier positif s inférieur à r et la clé publique est le point  $W=s.G$ . Le procédé de génération de la signature d'un message m comporte les 5 étapes suivantes:

- 10 1) Générer un nombre aléatoire u et calculer  $V=u.G$ .
- 2) Obtenir le message  $m'$  en enlevant au message m les t octets de poids faible et calculer  $f=R(m')$ .
- 15 3) Associer au point V un entier i et calculer  $c=i+f$  modulo r. Retourner à l'étape 1) si  $c=0$  ou si i n'est pas égal à m modulo  $2^t$ .
- 4) Calculer  $d=u-s*c$  modulo r.
- 5) La signature est la paire d'entiers  $(c, d)$ .

20

Le procédé de vérification de la signature comporte les 4 étapes suivantes:

- 1) Si c n'appartient pas à l'intervalle  $[1, r-1]$  25 ou si d n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide.
- 2) Calculer le point  $P=d.G+c.W$ . Si  $P=0$ , la signature n'est pas valide.
- 3) Associer au point P l'entier i et calculer 30 l'entier  $f=c-i$  modulo r.

4) Retrouver le message  $m'$  à partir de  $f$  et vérifier que  $f=R(m')$ . Si oui, retrouver le message  $m$  en concaténant au message  $m'$  les  $t$  octets de poids faible de  $i$ . La signature du 5 message  $m$  est alors valide. Sinon, la signature n'est pas valide.

Le septième procédé de l'invention consiste en une modification du schéma de signature avec ~~10 reconstitution partielle du message précédemment~~ décrit permettant d'augmenter de  $t$  octets la taille du message  $m_1$  reconstitué à partir de la signature,  $t$  étant une variable entière. Le septième procédé utilise une fonction de ~~15 redondance  $R$ , une courbe elliptique formant une structure de groupe dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ . Le procédé de génération de la signature d'un message  $m$ , constitué de deux messages  $m_1$  et  $m_2$ , comporte les 6 étapes suivantes:~~

- ~~25~~ 1) Générer un entier aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$
- 2) Obtenir  $m'_1$  en enlevant au message  $m_1$  les  $t$  octets de poids faible. Calculer  $f_1=R(m'_1)$
- 3) Associer au point  $V$  un entier  $i$  et calculer ~~30~~  $c=i+f_1$  modulo  $r$ . Si  $c=0$  ou si  $i$  n'est pas égal à  $m_1$  modulo  $2^{8t}$ , retourner à l'étape 1.

- 4) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage.
- 5) Calculer l'entier  $d=u^{-1} \cdot (f_2+s \cdot c) \pmod{r}$ . Si  $d=0$ , retourner à l'étape 1.
- 5 6) La signature est le couple d'entiers  $(c, d)$
- 

Le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c, d)$  et le message partiel  $m_2$  et comprend les 7 étapes 10 suivantes:

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.
- 15 2) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage.
- 3) Calculer les entiers  $h=d^{-1} \pmod{r}$ ,  $h_1=f_2 \cdot h \pmod{r}$  et  $h_2=c \cdot h \pmod{r}$ .
- 4) Calculer le point  $P=h_1G+h_2W$ . Si  $P=O$ , la 20 signature n'est pas valide.
- 5) Associer au point  $P$  l'entier  $i$ .
- 6) Calculer l'entier  $f_1=c-i \pmod{r}$ .
- 7) Obtenir le message  $m'_1$  à partir de  $f_1$  et vérifier que  $f_1=R(m'_1)$ . Si oui, obtenir  $m_1$  en 25 concaténant au message  $m'_1$  les  $t$  octets de poids faible de l'entier  $i$ . La signature du message  $m$  est alors valide. Sinon, la signature n'est pas valide.
- 30 Il est possible pour les sixièmes et septièmes procédés de diminuer les temps de calcul en

effectuant des prétraitements. Ces prétraitements consistent à mettre en mémoire dans une table des couples d'entiers  $(u, i)$  tels que définis précédemment de telle sorte que ces 5 entiers soient accessibles par la valeur de  $i$  modulo  $2^{8t}$ .

Le huitième procédé de l'invention consiste en une modification du schéma de signature de 10 Nyberg et Rueppel consistant à enlever  $t$  octets à l'entier  $c$  précédemment défini,  $t$  étant une variable entière. Le procédé de génération de signature comporte les 2 étapes suivantes:

15 1) Générer la signature  $s$  du message  $m$  en utilisant le schéma de signature de Nyberg-Rueppel pour obtenir le couple d'entiers  $(c, d)$ .  
 2) Calculer  $c'$ , quotient entier de la division de l'entier  $c$  par  $2^{8t}$ . La signature est le couple 20 d'entiers  $(c', d)$ .

Le procédé de vérification de signature prend en entrée le couple d'entiers  $(c', d)$  et comporte les 5 étapes suivantes:

25 1) Si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide.  
 2) Calculer le point  $P=d \cdot G + c'^{2^{8t}} \cdot W$   
 3) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les 30 étapes suivantes:  
 3)a) Si  $P=O$ , exécuter l'étape 3)d)

3)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$ .

3)c) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$ . Si oui, exécuter l'étape

5 5).

---

3)d) Remplacer  $P$  par  $P+W$ .

4) La signature n'est pas valide et le procédé est terminé.

5) Si l'entier  $c=c'*2^{8t}+j$  n'appartient pas à 10 l'intervalle  $[1, r-1]$ , la signature n'est pas valide, sinon la signature est valide et le procédé est terminé.

Le neuvième procédé de l'invention est une 15 modification du schéma de signature avec reconstitution partielle du message défini précédemment, qui consiste à enlever  $t$  octets de l'entier  $c$  défini précédemment,  $t$  étant une variable entière. Le procédé de génération de 20 signature comprend les 2 étapes suivantes:

1) Générer la signature du message  $m$ , constitué de deux messages  $m_1$  et  $m_2$ , en utilisant le schéma de signature avec reconstitution partielle du message pour obtenir le couple d'entiers  $(c, d)$ .

2) Calculer  $c'$ , quotient entier de la division de l'entier  $c$  par  $2^{8t}$ . La signature est le couple d'entiers  $(c', d)$ .

Le procédé de vérification de signature prend en entrée un couple d'entiers  $(c', d)$  et un message  $m_2$  et comprend les 8 étapes suivantes:

- 5 1) Si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.
- 2) Calculer  $f_2 = H(m_2)$ , où  $H$  est une fonction de hachage.
- 3) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  modulo  $r$  et  $h_2 = c' * 2^{8t} * h$  modulo  $r$ .
- 4) Calculer le point  $P = h_1 \cdot G + h_2 \cdot W$
- 5) Calculer le point  $Z = h \cdot W$ .
- 6) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les étapes suivantes:
  - 15 6)a) Si  $P=0$ , exécuter l'étape 6)d)
  - 6)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f_1 = c - i$  modulo  $r$ .
  - 6)c) Retrouver le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1 = R(m_1)$ . Si oui, exécuter l'étape 8).
  - 6)d) Remplacer  $P$  par  $P+Z$ .
- 7) La signature n'est pas valide et le procédé est terminé.
- 8) Si l'entier  $c = c' * 2^{8t} + j$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide, sinon la signature est valide et le procédé est terminé.

Le dixième procédé de l'invention consiste en une modification du schéma de signature avec reconstitution partielle du message précédemment

décrit, qui consiste à remplacer la signature  $(c, d)$  par la signature  $(h_2, d)$  avec  $h_2=c*d^{-1}$  modulo  $r$ . L'avantage de ce dixième procédé est de permettre une réduction du temps de calcul  
5 lorsque ce procédé est appliqué à l'un quelconque des procédés définis précédemment.

---

Le onzième procédé de l'invention consiste en une amélioration du schéma de signature de  
10 Nyberg-Rueppel rappelé précédemment, et consiste à inclure une partie du message de taille  $t$  octets dans l'entier  $d$  défini précédemment,  $t$  étant un entier petit, ainsi qu'à utiliser une autre fonction de redondance. Dans ce procédé,  
15 les  $t$  octets de poids faible de l'entier  $d$  contiennent  $t$  octets du message. Le onzième procédé utilise une courbe elliptique formant une structure de groupe dont l'élément zéro est noté  $O$  et un point  $G$  de la courbe, lequel point  
20  $G$  est générateur d'un sous-groupe d'ordre un nombre premier  $r$ . La clé privée est un entier positif  $s$  inférieur à  $r$  et la clé publique est le point  $W=s.G$ . Le procédé de génération de la signature d'un message  $m$  utilise les paramètres  
25 entiers  $t$ ,  $a$ , et  $k$  et comporte les 7 étapes suivantes:

- 1) Calculer  $h=H(m)$ ,  $H$  étant une fonction de hachage.

- 2) Enlever les  $t$  octets de poids faible et les  $k$  octets de poids fort du message  $m$  et mémoriser le résultat dans  $m'$ .
- 3) Mémoriser dans  $f$  le résultat de la concaténation à  $m'$  des  $a$  octets de poids fort de  $h$ .
- 4) Générer un nombre aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$ .
- 5) Associer au point  $V$  un entier  $i$  et calculer  
~~10 c=i+f modulo r. Retourner à l'étape 4) si c=0~~
- 6) Calculer l'entier  $d=u-s*c$  modulo  $r$ . Si  $d$  n'est pas égal à  $m$  modulo  $2^{8t}$  retourner à l'étape 4).
- 7) La signature est le couple d'entiers  $(c, d)$ .

15

Le procédé de vérification de la signature comporte les 7 étapes suivantes.

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide.
- 2) Calculer le point  $P=d.G+c.W$ . Si  $P=0$ , la signature n'est pas valide.
- 3) Associer au point  $P$  l'entier  $i$ .
- 4) Calculer l'entier  $f=c-i$  modulo  $r$ .
- 5) Concaténer au message  $m'$  obtenu à partir de  $f$  en enlevant les  $a$  octets de poids faible les  $t$  octets de poids faible de  $d$ .
- 6) Pour  $b$  allant de 0 à  $2^{8k}-1$  répéter l'étape 30 suivante :

6)a) Concaténer à  $b$  le message  $m'$  pour obtenir  $m$  et calculer  $h=H(m)$ . Vérifier que les  $a$  octets de poids fort de  $h$  et les  $a$  octets de poids faible de  $f$  sont identiques. Si oui, la signature du  
5 message  $m$  est valide et le procédé est terminé.

---

7) La signature n'est pas valide.

Les procédés décrits permettent donc de réduire de façon significative la taille totale de la  
10 signature et du message à transmettre. Lorsque la place en mémoire est limitée, il est ainsi possible de stocker un plus grand nombre de signatures. En outre, il est également possible de réaliser une transmission plus rapide des  
15 signatures. Ces procédés sont particulièrement destinées à être mises en place dans des dispositifs portables, par exemple de type carte à puce.

## REVENDICATIONS

1- Procédé de signature électronique comprenant un procédé de génération et un procédé de vérification permettant un reconstitution totale du message, ledit procédé utilisant une fonction de redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $0$  et de générateur le point  $G$ , la clé privée étant un entier positif inférieur à  $r$ , la clé publique étant le point  $W=s.G$ , ledit procédé utilisant une constante entière  $k$  non nulle, caractérisé en ce que le procédé de génération de signature comporte les 4 étapes suivantes:

15 1) Générer un nombre aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$ .

2) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$ . Si  $c=0$ , retourner à l'étape 1).

3) Calculer l'entier  $d=u^{-1}*(k+s*c)$  modulo  $r$ . Si  $d=0$ , retourner à l'étape 1).

4) La signature est la paire d'entiers  $(c,d)$ .

et en ce que le procédé de vérification de la signature comporte les 6 étapes suivantes:

25 1) Si  $c$  n'appartient pas à l'intervalle  $[1,r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1,r-1]$ , la signature n'est pas valide.

2) Calculer les entiers  $h=d^{-1}$  modulo  $r$ ,  $h_1=k*h$  modulo  $r$  et  $h_2=c*h$  modulo  $r$ .

- 3) Calculer le point  $P = h_1G + h_2W$ . Si  $P=O$ , la signature n'est pas valide.
- 4) Associer au point  $P$  un entier  $i$ .
- 5) Calculer l'entier  $f = c - i$  modulo  $r$ .
- 6) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f = R(m)$ . Si oui, la signature du message  $m$  est valide. Sinon, la signature n'est pas valide.

10

2- Procédé de signature électronique comprenant un procédé de génération et un procédé de vérification de signature permettant une reconstitution partielle du message, le message à signer étant divisé en 2 parties, la première partie  $m_1$  de taille constante étant reconstituée à partir de la signature, la deuxième partie  $m_2$  étant transmise avec la signature du message, ledit procédé utilisant une fonction de redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $O$  et de générateur le point  $G$ , la clé privée étant un entier positif inférieur à  $r$  et la clé publique étant le point  $W = s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message  $m$  constitué des messages  $m_1$  et  $m_2$  comporte les 6 étapes suivantes:

- 1) Générer un entier aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$
- 2) Calculer  $f_1=R(m_1)$
- 3) Associer au point  $V$  un entier  $i$  et calculer
- 5  $c=i+f_1$  modulo  $r$ . Si  $c=0$ , retourner à l'étape 1.
- 4) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage.
- 5) Calculer l'entier  $d=u^{-1} \cdot (f_2+s \cdot c)$  modulo  $r$ . Si  $d=0$ , retourner à l'étape 1.
- 10 6) La signature est le couple d'entiers  $(c, d)$

et en ce que le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c, d)$  et le message partiel  $m_2$  et comprend les 7 étapes suivantes:

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.
- 20 2) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage.
- 3) Calculer les entiers  $h=d^{-1}$  modulo  $r$ ,  $h_1=f_2 \cdot h$  modulo  $r$  et  $h_2=c \cdot h$  modulo  $r$ .
- 4) Calculer le point  $P=h_1G+h_2W$ . Si  $P=0$ , la signature n'est pas valide.
- 25 5) Associer au point  $P$  l'entier  $i$ .
- 6) Calculer l'entier  $f_1=c-i$  modulo  $r$ .
- 7) Obtenir le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1=R(m_1)$ . Si oui, la signature du

message  $m$  est valide. Sinon, la signature n'est pas valide.

---

3 - Procédé de signature électronique comprenant  
5 un procédé de génération et un procédé de vérification de signature caractérisé en ce qu'il consiste à inclure une partie du message à l'intérieur de la signature en choisissant convenablement les données aléatoires utilisées  
10 lors de la génération de la signature.

4 - Procédé de signature électronique comprenant un procédé de génération et un procédé de vérification de signature caractérisé en ce  
15 qu'il consiste à supprimer une partie des octets représentant la signature, la reconstitution complète de la signature s'effectuant durant la phase de vérification.

20 5 - Procédé d'amélioration du schéma de signature de Nyberg-Rueppel selon la revendication 3 comprenant un procédé de génération et un procédé de vérification et consistant à inclure une partie du message de taille  $t$  octets dans  
25 l'entier  $d$ ,  $t$  étant un entier petit, la signature étant le couple d'entiers  $(c,d)$ , les  $t$  octets de poids faible de l'entier  $d$  contenant  $t$  octets du message, ledit procédé utilisant une fonction de redondance  $R$ , un ensemble possédant

une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $O$  et de générateur le point  $G$ , la clé privée étant un entier positif  $s$  inférieur à  $r$  et la clé 5 publique étant le point  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message  $m$  comporte les 5 étapes suivantes:

- 1) Enlever les  $t$  octets de poids faible du 10 message  $m$  et mémoriser le résultat dans  $m'$ . Calculer  $f=R(m')$ .
- 2) Générer un nombre aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$ .
- 3) Associer au point  $V$  un entier  $i$  et calculer 15  $c=i+f$  modulo  $r$ . Retourner à l'étape 1) si  $c=0$ .
- 4) Calculer l'entier  $d=u-s*c$  modulo  $r$ . Si  $d$  n'est pas égal à  $m$  modulo  $2^8$  retourner à l'étape 2).
- 5) La signature est le couple d'entiers  $(c, d)$ .

20

et en ce que le procédé de vérification de la signature comporte les 5 étapes suivantes:

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  25 ou si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide.
- 2) Calculer le point  $P=d.G+c.W$ . Si  $P=O$ , la signature n'est pas valide.
- 3) Associer au point  $P$  l'entier  $i$ .

- 4) Calculer l'entier  $f=c-i$  modulo  $r$ .
- 5) Obtenir le message  $m'$  à partir de  $f$  et vérifier que  $f=R(m')$ . Si ce n'est pas le cas, la signature n'est pas valide. Si c'est le cas, la
- 
- 5 signature est valide et le message  $m$  est la concaténation au message  $m'$  des  $t$  octets de poids faible de l'entier  $d$ .
- 10 6- Procédé de prétraitement de la génération de signature selon la revendication 5 permettant d'accélérer la génération des signatures, ledit procédé comprenant une phase de prétraitement et une phase de génération de la signature, ladite
- 15 phase de prétraitement prenant en entrée la clé secrète  $s$  et consistant à mettre en mémoire dans une table un grand nombre de valeurs  $(i, x_u)$  avec  $x_u=u-s*i$  modulo  $r$  et  $i$  étant l'entier associé au point  $V=u.G$ , de telle sorte que ces
- 20 valeurs puissent être accédées par le reste de  $x_u$  modulo  $2^{8t}$ , ladite phase de génération de signature utilisant une fonction de redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté
- 25 0 et de générateur le point  $G$ , la clé privée étant un entier positif  $s$  inférieur à  $r$  et la clé publique étant le point  $W=s.G$ , ladite phase de génération de la signature étant caractérisé par les 8 étapes suivantes:

- 1) Enlever les  $t$  octets de poids faible du message  $m$  et mémoriser le résultat dans  $m'$ .  
 Calculer  $f=R(m')$ . Les  $t$  octets de poids faible du message  $m$  sont mémorisés dans l'entier  $\delta$ .
- 5 2) Calculer l'entier  $y=s*f$  modulo  $r$  et l'entier  $\lambda=y$  modulo  $2^{8t}$ .
- 3) Si  $y < r/2$ , exécuter d'abord l'étape 4 et ensuite l'étape 5, sinon exécuter d'abord 10 l'étape 5 et ensuite l'étape 4.
- 4) Accéder aux éléments de la table dont le reste modulo  $2^{8t}$  est  $\lambda+\delta$  modulo  $2^{8t}$  et sélectionner un élément tel que  $x_u$  est supérieur ou égal à  $y$ . Si un tel élément existe, il est 15 supprimé de la table et le procédé passe à l'étape 6)
- 5) Accéder aux éléments de la table dont le reste modulo  $2^{8t}$  est  $\lambda+\delta+r$  modulo  $2^{8t}$  et sélectionner un élément tel que  $x_u$  est inférieur 20 à  $y$ . Si un tel élément existe, il est supprimé de la table et le procédé passe à l'étape 6)
- 6) Calculer l'entier  $d = x_u - y$  modulo  $r$ .
- 7) Obtenir l'entier  $i$  associé à  $x_u$  et calculer  $c = i + f$  modulo  $r$ .
- 25 8) La signature est le couple d'entiers  $(c, d)$ .

7- Procédé d'amélioration du schéma de signature avec reconstitution partielle du message selon

la revendication 2, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, ledit procédé consistant à inclure une partie du 5 message de taille  $t$  octets dans l'entier  $d$  défini précédemment,  $t$  étant un entier petit, les  $t$  octets de poids faible de l'entier  $d$  contenant  $t$  octets du message, ledit procédé utilisant une fonction de redondance  $R$ , un 10 ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $O$  et de générateur le point  $G$ , la clé privée étant un entier positif inférieur à  $r$  et la clé publique étant le point  $W=s.G$ , caractérisé en ce 15 que le procédé de génération de la signature d'un message  $m$  constitué des messages  $m_1$  et  $m_2$  comporte les 6 étapes suivantes:

- 1) Générer un entier aléatoire  $u$  compris entre 1 20 et  $r-1$  et calculer  $V=u.G$
- 2) Calculer  $f_1=R(m_1)$
- 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f_1$  modulo  $r$ . Si  $c=0$ , retourner à l'étape 1.
- 4) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de 25 hachage.
- 5) Calculer l'entier  $d=u^{-1}*(f_2+s*c)$  modulo  $r$ . Si  $d=0$  ou si  $d$  n'est pas égal à  $m_2$  modulo  $2^{8t}$  retourner à l'étape 1).

6) La signature est le couple d'entiers  $(c, d)$  et le message à transmettre est  $m'_2$  consistant en  $m_2$  privé de ses  $t$  octets de poids faible.

5 et en ce que le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c, d)$  et le message partiel  $m'_2$ , et comprend les 8 étapes suivantes:

- 10 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.
- 2) Compléter  $m'_2$  en  $m_2$  en lui ajoutant les  $t$  octets de poids faible de  $d$ .
- 15 3) Calculer  $f_2 = H(m_2)$ , où  $H$  est une fonction de hachage.
- 4) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  modulo  $r$  et  $h_2 = c * h$  modulo  $r$ .
- 5) Calculer le point  $P = h_1 G + h_2 W$ . Si  $P = O$ , la signature n'est pas valide.
- 20 6) Associer au point  $P$  l'entier  $i$ .
- 7) Calculer l'entier  $f_1 = c - i$  modulo  $r$ .
- 8) Obtenir le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1 = R(m_1)$ . Si oui, la signature du message  $m$  est valide. Sinon, la signature n'est pas valide.

8- Procédé consistant à enlever  $t$  octets de la chaîne d'octets représentant l'entier  $d$  lorsque

la signature est le couple d'entiers  $(c, d)$ , ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, ledit procédé 5 s'appliquant au schéma de signature de Nyberg et Rueppel, caractérisé en ce que le procédé modifié de génération de signature comporte les 2 étapes suivantes:

- 10 1) Générer la signature du message  $m$  en utilisant le schéma de signature de Nyberg et Rueppel, pour obtenir le couple d'entiers  $(c, d)$ .  
2) Calculer  $d'$ , quotient entier de la division de l'entier  $d$  par  $2^{st}$ . La signature est le couple 15 d'entiers  $(c, d')$ .

et en ce que le procédé modifié de vérification de signature prend en entrée un couple  $(c, d')$  et comporte les 5 étapes suivantes :  
20  
1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.  
2) Calculer le point  $P=d'*2^{st}.G+c.W$   
3) Pour  $j$  allant de 0 à  $2^{st}-1$ , exécuter les 25 étapes suivantes:  
3)a) Si  $P=0$ , exécuter l'étape 3)d)  
3)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$ .

3)c) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$ . Si oui, exécuter l'étape 5).

3)d) Remplacer  $P$  par  $P+G$ .

5 4) La signature n'est pas valide et le procédé est terminé.

5) Si l'entier  $d=d'*2^{8t}+j$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide, sinon la signature est valide et le 10 procédé est terminé.

8bis- Procédé consistant à enlever  $t$  octets de la chaîne d'octets représentant l'entier  $d$  lorsque la signature est le couple d'entiers 15  $(c, d)$ , ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, ledit procédé au schéma de signature avec reconstitution partielle du message selon la revendication 2, 20 caractérisé en ce que le procédé modifié de génération de signature comporte les 2 étapes suivantes:

1) Générer la signature du message  $m$  en 25 utilisant le schéma de signature avec reconstitution partielle du message précédemment décrit, pour obtenir le couple d'entiers  $(c, d)$ .

2) Calculer  $d'$ , quotient entier de la division de l'entier  $d$  par  $2^{8t}$ . La signature est le couple d'entiers  $(c, d')$ .

5 et en ce que le procédé modifié de vérification de signature prend en entrée un couple  $(c, d')$  et un message  $m_2$  et comporte les 2 étapes suivantes :

10 1) Pour  $i$  allant de 0 à  $2^{8t}-1$ , calculer l'entier  $d=d'*2^{8t}+i$  et exécuter le procédé de vérification de signature avec reconstitution partielle du message précédemment décrit, la signature à vérifier étant  $(c, d)$ . Si le procédé de vérification de signature reconnaît la signature  $(c, d)$  comme valide, la signature est valide, et le procédé est terminé.

15 2) La signature n'est pas valide.

20 9- Procédé d'amélioration du schéma de Nyberg et Rueppel permettant d'augmenter de  $t$  octets la taille des messages à signer,  $t$  étant une variable entière, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, ledit procédé utilisant une fonction de redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté 0 et de générateur le point  $G$ , la clé privée

étant un entier positif  $s$  inférieur à  $r$  et la clé publique étant le point  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message  $m$  comporte les 5 étapes suivantes:

- 1) Générer un nombre aléatoire  $u$  et calculer  $V=u.G$ .
- 2) Obtenir le message  $m'$  en enlevant au message  $m$  les  $t$  octets de poids faible et calculer  $f=R(m')$ .
- 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$ . Retourner à l'étape 1) si  $c=0$  ou si  $i$  n'est pas égal à  $m$  modulo  $2^t$ .
- 4) Calculer  $d=u*s*c$  modulo  $r$ .
- 5) La signature est la paire d'entiers  $(c, d)$ .

et en ce que le procédé de vérification de la signature comporte les 4 étapes suivantes:

- 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide.
- 2) Calculer le point  $P=d.G+c.W$ . Si  $P=0$ , la signature n'est pas valide.
- 3) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$ .
- 4) Retrouver le message  $m'$  à partir de  $f$  et vérifier que  $f=R(m)$ . Si oui, retrouver le

message  $m$  en concaténant au message  $m'$  les  $t$  octets de poids faible de  $i$ . La signature du message  $m$  est alors valide. Sinon, la signature n'est pas valide.

5

10- Procédé d'amélioration du schéma de signature avec reconstitution partielle du message selon la revendication 2, ledit procédé comprenant un procédé de génération de la 10 signature et un procédé de vérification de la signature, ledit procédé permettant d'augmenter de  $t$  octets la taille du message  $m_1$  reconstitué à partir de la signature,  $t$  étant une variable entière, ledit procédé utilisant une fonction de 15 redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $0$  et de générateur le point  $G$ , la clé privée étant un entier positif inférieur à  $r$  et la clé publique étant le point 20  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message  $m$  comporte les 6 étapes suivantes :

- 1) Générer un entier aléatoire  $u$  compris entre 1 25 et  $r-1$  et calculer  $V=u.G$
- 2) Obtenir  $m'_1$  en enlevant au message  $m_1$  les  $t$  octets de poids faible. Calculer  $f_1=R(m'_1)$

- 3) Associer au point  $V$  un entier  $i$  et calculer  $c = i + f_1$  modulo  $r$ . Si  $c=0$  ou si  $i$  n'est pas égal à  $m_1$  modulo  $2^{8t}$ , retourner à l'étape 1.
  - 4) Calculer  $f_2 = H(m_2)$ , où  $H$  est une fonction de hachage.
  - 5) Calculer l'entier  $d = u^{-1} * (f_2 + s * c)$  modulo  $r$ . Si  $d=0$ , retourner à l'étape 1.
  - 6) La signature est le couple d'entiers  $(c, d)$ .
- 10 et en ce que le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c, d)$  et le message partiel  $m_2$  et comprend les 7 étapes suivantes :
- 15 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.
  - 2) Calculer  $f_2 = H(m_2)$ , où  $H$  est une fonction de hachage.
  - 20 3) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  modulo  $r$  et  $h_2 = c * h$  modulo  $r$ .
  - 4) Calculer le point  $P = h_1 G + h_2 W$ . Si  $P=0$ , la signature n'est pas valide.
  - 5) Associer au point  $P$  l'entier  $i$ .
  - 25 6) Calculer l'entier  $f_1 = c - i$  modulo  $r$ .
  - 7) Obtenir le message  $m'_1$  à partir de  $f_1$  et vérifier que  $f_1 = R(m'_1)$ . Si oui, obtenir  $m_1$  en concaténant au message  $m'_1$  les  $t$  octets de poids faible de l'entier  $i$ . La signature du message  $m$

est alors valide. Sinon, la signature n'est pas valide.

---

5 11- Procédé de prétraitement des calculs permettant d'augmenter les performances des procédés selon les revendications 9 et 10, caractérisé en ce qu'il consiste à mettre en mémoire dans une table des couples d'entiers 10  $(u, i)$  de telle sorte que ces entiers soient accessibles par la valeur de  $i$  modulo  $2^s t$ ,  $t$  étant un paramètre entier.

12- Procédé d'amélioration du schéma de 15 signature de Nyberg et Rueppel consistant à enlever  $t$  octets à l'entier  $c$ ,  $t$  étant une variable entière, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, la 20 signature étant constitué du couple d'entiers  $(c, d)$ , caractérisé en ce que le procédé de génération de signature comporte les 2 étapes suivantes:

25 1) Générer la signature du message  $m$  en utilisant le schéma de signature de Nyberg-Rueppel pour obtenir le couple d'entiers  $(c, d)$ .

2) Calculer  $c'$ , quotient entier de la division de l'entier  $c$  par  $2^{8t}$ . La signature est le couple d'entiers  $(c', d)$ .

5 et en ce que le procédé de vérification de signature prend en entrée le couple d'entiers  $(c', d)$  et comporte les 5 étapes suivantes:

- 1) Si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ ,  
10 la signature n'est pas valide.
- 2) Calculer le point  $P=d.G+c' * 2^{8t}.W$
- 3) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les étapes suivantes:
  - 3)a) Si  $P=0$ , exécuter l'étape 3)d).
  - 15 3)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$ .
  - 3)c) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$ . Si oui, exécuter l'étape 5).
  - 20 3)d) Remplacer  $P$  par  $P+W$ .
- 4) La signature n'est pas valide et le procédé est terminé.
- 5) Si l'entier  $c=c'*2^{8t}+j$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide, sinon la signature est valide et le procédé est terminé.

13- Procédé d'amélioration du schéma de signature avec reconstitution partielle du

message selon la revendication 2 consistant à enlever  $t$  octets de l'entier  $c$  défini selon la revendication 2,  $t$  étant une variable entière, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, caractérisé en ce que le procédé de génération de signature comprend les 2 étapes suivantes:

- 10 1) Générer la signature du message  $m$  en utilisant le schéma de signature avec reconstitution partielle du message pour obtenir le couple d'entiers  $(c, d)$ .
- 2) Calculer  $c'$ , quotient entier de la division de l'entier  $c$  par  $2^{8t}$ . La signature est le couple d'entiers  $(c', d)$ .

et en ce que le procédé de vérification de signature prend en entrée un couple d'entiers  $(c', d)$  et un message  $m_2$  et comprend les 8 étapes suivantes:

- 1) Si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.
- 25 2) Calculer  $f_2 = H(m_2)$ , où  $H$  est une fonction de hachage.
- 3) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  modulo  $r$  et  $h_2 = c' * 2^{8t} * h$  modulo  $r$ .
- 4) Calculer le point  $P = h_1 \cdot G + h_2 \cdot W$

- 5) Calculer le point  $Z=h.W$ .
- 6) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les étapes suivantes:
  - 6)a) Si  $P=0$ , exécuter l'étape 6)d)
  - 6)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f_1=c-i$  modulo  $r$ .
  - 6)c) Retrouver le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1=R(m_1)$ . Si oui, exécuter l'étape 8).
  - 6)d) Remplacer  $P$  par  $P+Z$ .
- 7) La signature n'est pas valide et le procédé est terminé.
- 8) Si l'entier  $c=c'*2^{8t}+j$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide, sinon la signature est valide et le procédé est terminé.

14- Procédé de modification du schéma de signature avec reconstitution partielle du message selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste à remplacer la signature  $(c, d)$  par la signature  $(h_2, d)$  avec  $h_2=c*d^{-1}$  modulo  $r$ .

15 - Procédé d'amélioration du schéma de signature de Nyberg-Rueppel, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la

signature, ledit procédé consistant à inclure une partie du message de taille  $t$  octets dans l'entier  $d$ , la signature étant le couple d'entiers  $(c, d)$ ,  $t$  étant un entier petit, les  $t$  5 octets de poids faible de l'entier  $d$  contenant  $t$  octets du message, ledit procédé utilisant un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $O$  et de générateur le point  $G$ , la clé privée 10 étant un entier positif  $s$  inférieur à  $r$  et la clé publique étant le point  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message  $m$  utilisant les paramètres entiers  $t$ ,  $a$ , et  $k$  et comporte les 7 15 étapes suivantes:

- 1) Calculer  $h=H(m)$ ,  $H$  étant une fonction de hachage.
- 2) Enlever les  $t$  octets de poids faible et les  $k$  20 octets de poids fort du message  $m$  et mémoriser le résultat dans  $m'$ .
- 3) Mémoriser dans  $f$  le résultat de la concaténation à  $m'$  des  $a$  octets de poids fort de  $h$ .
- 25 4) Générer un nombre aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$ .
- 5) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$ . Retourner à l'étape 4) si  $c=0$

6) Calculer l'entier  $d=u-s*c$  modulo  $r$ . Si  $d$  n'est pas égal à  $m$  modulo  $2^{8t}$  retourner à l'étape 4).

7) La signature est le couple d'entiers  $(c, d)$ .

5

et en ce que le procédé de vérification de la signature comporte les 7 étapes suivantes:

1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  10 ou si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide.

2) Calculer le point  $P=d.G+c.W$ . Si  $P=0$ , la signature n'est pas valide.

3) Associer au point  $P$  l'entier  $i$ .

15 4) Calculer l'entier  $f = c.i$  modulo  $r$ .

5) Concaténer au message  $m'$ , obtenu à partir de  $f$  en enlevant les a octets de poids faible, les t octets de poids faible de  $d$ .

6) Pour  $b$  allant de 0 à  $2^{8k}-1$  répéter l'étape 20 suivante :

6)a) Concaténer à  $b$  le message  $m'$  pour obtenir  $m$  et calculer  $h=H(m)$ . Vérifier que les a octets de poids fort de  $h$  et les a octets de poids faible de  $f$  sont identiques. Si oui, la signature du 25 message  $m$  est valide et le procédé est terminé.

7) La signature n'est pas valide.

16- Procédé de génération et de vérification de signature électronique selon l'une quelconque

des revendications précédentes caractérisé en ce que les opérations s'effectuent sur une courbe elliptique formant une structure de groupe et possédant au moins un point  $G$ , qui est 5 générateur d'un sous-groupe d'ordre un nombre premier  $r$ .

17- Procédé de génération et de vérification de signature électronique selon l'une quelconque 10 des revendications précédentes caractérisé en ce que les opérations s'effectuent dans le groupe multiplicatif des entiers modulo un nombre premier  $p$ .

15 18- Procédé de génération et de vérification de signature électronique selon l'une quelconque des revendications précédentes caractérisé en ce que les opérations s'effectuent dans un sous-groupe multiplicatif d'ordre un entier premier  $r$  20 du groupe multiplicatif des entiers modulo un nombre premier  $p$  avec  $r$  divisant  $p-1$ .

19. Dispositif électronique selon l'une quelconque des revendications précédentes 25 caractérisé en ce que le dispositif effectuant le test est un dispositif portable.

20. Dispositif électronique selon l'une quelconque des revendications précédentes

caractérisé en ce que le dispositif est une carte à puce.

---

21. Dispositif électronique selon l'une  
5 quelconque des revendications précédentes  
caractérisé en ce que le dispositif est une  
carte sans contact.

---

22. Dispositif électronique selon l'une  
10 quelconque des revendications précédentes  
caractérisé en ce que le dispositif est une  
carte ~~PCMCI A~~.

23. Dispositif électronique selon l'une  
15 quelconque des revendications précédentes  
caractérisé en ce que le dispositif est un  
badge.

24. Dispositif électronique selon l'une  
20 quelconque des revendications précédentes  
caractérisé en ce que le dispositif est une  
montre intelligente.

3)c) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$ . Si oui, exécuter l'étape 5).

~~3)d) Remplacer  $P$  par  $P+G$ .~~

5 4) La signature n'est pas valide et le procédé est terminé.

5) Si l'entier  $d=d'*2^{8t}+j$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide, sinon la signature est valide et le 10 procédé est terminé.

9- Procédé consistant à enlever  $t$  octets de la chaîne d'octets représentant l'entier  $d$  lorsque la signature est le couple d'entiers  $(c, d)$ , 15 ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, ledit procédé au schéma de signature avec reconstitution partielle du message selon la revendication 2, 20 caractérisé en ce que le procédé modifié de génération de signature comporte les 2 étapes suivantes:

1) Générer la signature du message  $m$  en 25 utilisant le schéma de signature avec reconstitution partielle du message précédemment décrit, pour obtenir le couple d'entiers  $(c, d)$  ;

2) Calculer  $d'$ , quotient entier de la division de l'entier  $d$  par  $2^{8t}$ . La signature est le couple d'entiers  $(c, d')$ .

5 et en ce que le procédé modifié de vérification de signature prend en entrée un couple  $(c, d')$  et un message  $m_2$  et comporte les 2 étapes suivantes :

10 1) Pour  $i$  allant de 0 à  $2^{8t}-1$ , calculer l'entier  $d=d'*2^{8t}+i$  et exécuter le procédé de vérification de signature avec reconstitution partielle du message précédemment décrit, la signature à vérifier étant  $(c, d)$ . Si le procédé de vérification de signature reconnaît la signature  $(c, d)$  comme valide, la signature est valide, et le procédé est terminé.

15 2) La signature n'est pas valide.

20 10- Procédé d'amélioration du schéma de Nyberg et Rueppel permettant d'augmenter de  $t$  octets la taille des messages à signer,  $t$  étant une variable entière, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, ledit procédé utilisant une fonction de redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté 0  
25 et de générateur le point  $G$ , la clé privée

étant un entier positif  $s$  inférieur à  $r$  et la clé publique étant le point  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message  $m$  comporte les 5 étapes

---

5 suivantes:

- 1) Générer un nombre aléatoire  $u$  et calculer  $V=u.G$ .
- 2) Obtenir le message  $m'$  en enlevant au message 10  $m$  les  $t$  octets de poids faible et calculer  $f=R(m')$ .
- 3) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$ . Retourner à l'étape 1) si  $c=0$  ou si  $i$  n'est pas égal à  $m$  modulo  $2^{8t}$ .
- 15 4) Calculer  $d=u-s*c$  modulo  $r$ .
- 5) La signature est la paire d'entiers  $(c, d)$ .

et en ce que le procédé de vérification de la signature comporte les 4 étapes suivantes:

- 20 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide.
- 2) Calculer le point  $P=d.G+c.W$ . Si  $P=0$ , la 25 signature n'est pas valide.
- 3) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$ .
- 4) Retrouver le message  $m'$  à partir de  $f$  et vérifier que  $f=R(m)$ . Si oui, retrouver le

message  $m$  en concaténant au message  $m'$  les  $t$  octets de poids faible de  $i$ . La signature du message  $m$  est alors valide. Sinon, la signature n'est pas valide.

5

11- Procédé d'amélioration du schéma de signature avec reconstitution partielle du message selon la revendication 2, ledit procédé comprenant un procédé de génération de la 10 signature et un procédé de vérification de la signature, ledit procédé permettant d'augmenter de  $t$  octets la taille du message  $m'$  reconstitué à partir de la signature,  $t$  étant une variable entière, ledit procédé utilisant une fonction de 15 redondance  $R$ , un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté  $0$  et de générateur le point  $G$ , la clé privée étant un entier positif inférieur à  $r$  et la clé publique étant le point 20  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message  $m$  comporte les 6 étapes suivantes :

- 1) Générer un entier aléatoire  $u$  compris entre 1 25 et  $r-1$  et calculer  $V=u.G$
- 2) Obtenir  $m'_1$  en enlevant au message  $m_1$  les  $t$  octets de poids faible. Calculer  $f_1=R(m'_1)$

- 3) Associer au point  $V$  un entier  $i$  et calculer  $c = i + f_1$  modulo  $r$ . Si  $c=0$  ou si  $i$  n'est pas égal à  $m_1$  modulo  $2^{8t}$ , retourner à l'étape 1.
  - 4) ~~Calculer  $f_2 = H(m_2)$ , où  $H$  est une fonction de hachage.~~
  - 5) Calculer l'entier  $d = u^{-1} * (f_2 + s * c)$  modulo  $r$ . Si  $d=0$ , retourner à l'étape 1.
  - 6) La signature est le couple d'entiers  $(c, d)$
- 10 et en ce que le procédé de vérification de la signature prend en entrée une paire d'entiers  $(c, d)$  et le message partiel  $m_2$  et comprend les 7 étapes suivantes:
- 15 1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  ou si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.
  - 2) ~~Calculer  $f_2 = H(m_2)$ , où  $H$  est une fonction de hachage.~~
  - 20 3) Calculer les entiers  $h = d^{-1}$  modulo  $r$ ,  $h_1 = f_2 * h$  modulo  $r$  et  $h_2 = c * h$  modulo  $r$ .
  - 4) Calculer le point  $P = h_1 G + h_2 W$ . Si  $P=0$ , la signature n'est pas valide.
  - 5) Associer au point  $P$  l'entier  $i$ .
  - 25 6) Calculer l'entier  $f_1 = c - i$  modulo  $r$ .
  - 7) Obtenir le message  $m'_1$  à partir de  $f_1$  et vérifier que  $f_1 = R(m'_1)$ . Si oui, obtenir  $m_1$  en concaténant au message  $m'_1$  les  $t$  octets de poids faible de l'entier  $i$ . La signature du message  $m$

est alors valide. Sinon, la signature n'est pas valide.

12- Procédé de prétraitement des calculs  
5 permettant d'augmenter les performances des procédés selon les revendications 10 et 11, caractérisé en ce qu'il consiste à mettre en mémoire dans une table des couples d'entiers  $(u, i)$  de telle sorte que ces entiers soient  
10 accessibles par la valeur de  $i$  modulo  $2^{8t}$ ,  $t$  étant un paramètre entier.

13- Procédé d'amélioration du schéma de signature de Nyberg et Rueppel consistant à  
15 enlever  $t$  octets à l'entier  $c$ ,  $t$  étant une variable entière, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, la signature étant constitué du couple d'entiers  
20  $(c, d)$ , caractérisé en ce que le procédé de génération de signature comporte les 2 étapes suivantes:

1) Générer la signature du message  $m$  en  
25 utilisant le schéma de signature de Nyberg-Rueppel pour obtenir le couple d'entiers  $(c, d)$ .

2) Calculer  $c'$ , quotient entier de la division de l'entier  $c$  par  $2^{8t}$ . La signature est le couple d'entiers  $(c', d)$ .

5 et en ce que le procédé de vérification de signature prend en entrée le couple d'entiers  $(c', d)$  et comporte les 5 étapes suivantes:

- 1) Si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ ,  
10 la signature n'est pas valide.
- 2) Calculer le point  $P=d.G+c' * 2^{8t}.W$
- 3) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les étapes suivantes:
  - 3)a) Si  $P=0$ , exécuter l'étape 3)d)
  - 15 3)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f=c-i$  modulo  $r$ .
  - 3)c) Retrouver le message  $m$  à partir de  $f$  et vérifier que  $f=R(m)$ . Si oui, exécuter l'étape 5).
  - 20 3)d) Remplacer  $P$  par  $P+W$ .
  - 4) La signature n'est pas valide et le procédé est terminé.
  - 5) Si l'entier  $c=c'*2^{8t}+j$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas  
25 valide, sinon la signature est valide et le procédé est terminé.

14- Procédé d'amélioration du schéma de signature avec reconstitution partielle du

message selon la revendication 2 consistant à enlever  $t$  octets de l'entier  $c$  défini selon la revendication 2,  $t$  étant une variable entière, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la signature, caractérisé en ce que le procédé de génération de signature comprend les 2 étapes suivantes:

- 10 1) Générer la signature du message  $m$  en utilisant le schéma de signature avec reconstitution partielle du message pour obtenir le couple d'entiers  $(c, d)$ .
- 2) Calculer  $c'$ , quotient entier de la division de l'entier  $c$  par  $2^{8t}$ . La signature est le couple d'entiers  $(c', d)$ .

et en ce que le procédé de vérification de signature prend en entrée un couple d'entiers  $(c', d)$  et un message  $m_2$  et comprend les 8 étapes suivantes:

- 1) Si  $d$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas valide.
- 25 2) Calculer  $f_2=H(m_2)$ , où  $H$  est une fonction de hachage.
- 3) Calculer les entiers  $h=d^{-1}$  modulo  $r$ ,  $h_1=f_2*h$  modulo  $r$  et  $h_2=c'*2^{8t}*h$  modulo  $r$ .
- 3) Calculer le point  $P= h_1.G+ h_2.W$

- 5) Calculer le point  $Z=h.W$ .
- 6) Pour  $j$  allant de 0 à  $2^{8t}-1$ , exécuter les étapes suivantes:
  - 6)a) ~~Si  $P=0$ , exécuter l'étape 6)d)~~
  - 6)b) Associer au point  $P$  l'entier  $i$  et calculer l'entier  $f_1=c-i$  modulo  $r$ .
  - 6)c) Retrouver le message  $m_1$  à partir de  $f_1$  et vérifier que  $f_1=R(m_1)$ . Si oui, exécuter l'étape 8).
  - 10 6)d) Remplacer  $P$  par  $P+Z$ .
  - 7) La signature n'est pas valide et le procédé est terminé.
  - 8) Si l'entier  $c=c'*2^{8t}+j$  n'appartient pas à l'intervalle  $[1, r-1]$ , la signature n'est pas 15 valide, sinon la signature est valide et le procédé est terminé.
- 15- Procédé de modification du schéma de 20 signature avec reconstitution partielle du message selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il consiste à remplacer la signature  $(c, d)$  par la signature  $(h_2, d)$  avec  $h_2=c*d^{-1}$  modulo  $r$ .
- 25 16- Procédé d'amélioration du schéma de signature de Nyberg-Rueppel, ledit procédé comprenant un procédé de génération de la signature et un procédé de vérification de la
- 30

signature, ledit procédé consistant à inclure une partie du message de taille  $t$  octets dans l'entier  $d$ , la signature étant le couple d'entiers  $(c,d)$ ,  $t$  étant un entier petit, les  $t$  5 octets de poids faible de l'entier  $d$  contenant  $t$  octets du message, ledit procédé utilisant un ensemble possédant une structure de groupe d'ordre un nombre premier  $r$ , d'élément zéro noté 0 et de générateur le point  $G$ , la clé privée 10 étant un entier positif  $s$  inférieur à  $r$  et la clé publique étant le point  $W=s.G$ , caractérisé en ce que le procédé de génération de la signature d'un message  $m$  utilisant les paramètres entiers  $t, a$ , et  $k$  et comporte les 15 étapes suivantes:

- 1) Calculer  $h=H(m)$ ,  $H$  étant une fonction de hachage.
- 2) Enlever les  $t$  octets de poids faible et les  $k$  20 octets de poids fort du message  $m$  et mémoriser le résultat dans  $m'$ .
- 3) Mémoriser dans  $f$  le résultat de la concaténation à  $m'$  des  $a$  octets de poids fort de  $h$ .
- 25 4) Générer un nombre aléatoire  $u$  compris entre 1 et  $r-1$  et calculer  $V=u.G$ .
- 4) Associer au point  $V$  un entier  $i$  et calculer  $c=i+f$  modulo  $r$ . Retourner à l'étape 4) si  $c=0$

6) Calculer l'entier  $d=u-s*c$  modulo  $r$ . Si  $d$  n'est pas égal à  $m$  modulo  $2^{8t}$  retourner à l'étape 4).

7) La signature est le couple d'entiers  $(c, d)$ .

5

et en ce que le procédé de vérification de la signature comporte les 7 étapes suivantes:

1) Si  $c$  n'appartient pas à l'intervalle  $[1, r-1]$  10 ou si  $d$  n'appartient pas à l'intervalle  $[0, r-1]$ , la signature n'est pas valide.

2) Calculer le point  $P=d.G+c.W$ . Si  $P=0$ , la signature n'est pas valide.

3) Associer au point  $P$  l'entier  $i$ .

15 4) Calculer l'entier  $f=c-i$  modulo  $r$ .

5) Concaténer au message  $m'$ , obtenu à partir de  $f$  en enlevant les  $a$  octets de poids faible, les  $t$  octets de poids faible de  $d$ .

6) Pour  $b$  allant de 0 à  $2^{8k}-1$  répéter l'étape 20 suivante :

6)a) Concaténer à  $b$  le message  $m'$  pour obtenir  $m$  et calculer  $h=H(m)$ . Vérifier que les  $a$  octets de poids fort de  $h$  et les  $a$  octets de poids faible de  $f$  sont identiques. Si oui, la signature du 25 message  $m$  est valide et le procédé est terminé.

7) La signature n'est pas valide.

17- Procédé de génération et de vérification de signature électronique selon l'une quelconque

des revendications précédentes caractérisé en ce que les opérations s'effectuent sur une courbe elliptique formant une structure de groupe et possédant au moins un point  $G$ , qui est 5 générateur d'un sous-groupe d'ordre un nombre premier  $r$ .

18- Procédé de génération et de vérification de signature électronique selon l'une quelconque 10 des revendications précédentes caractérisé en ce que les opérations s'effectuent dans le groupe multiplicatif des entiers modulo un nombre premier  $p$ .

15 19- Procédé de génération et de vérification de signatures électroniques selon l'une quelconque des revendications précédentes caractérisé en ce que les opérations s'effectuent dans un sous-groupe multiplicatif d'ordre un entier premier  $r$  20 du groupe multiplicatif des entiers modulo un nombre premier  $p$  avec  $r$  divisant  $p-1$ .

20. Dispositif électronique selon l'une quelconque des revendications précédentes 25 caractérisé en ce que le dispositif effectuant le test est un dispositif portable.

21. Dispositif électronique selon l'une quelconque des revendications précédentes

30

caractérisé en ce que le dispositif est une carte à puce.

22. Dispositif électronique selon l'une  
5 quelconque des revendications précédentes  
caractérisé en ce que le dispositif est une  
carte sans contact.

23. Dispositif électronique selon l'une  
10 quelconque des revendications précédentes  
caractérisé en ce que le dispositif est une  
carte PCMCIA.

24. Dispositif électronique selon l'une  
15 quelconque des revendications précédentes  
caractérisé en ce que le dispositif est un  
badge.

25. Dispositif électronique selon l'une  
20 quelconque des revendications précédentes  
caractérisé en ce que le dispositif est une  
montre intelligente.

This Page Blank (uspto)

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER: \_\_\_\_\_**

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

This Page Blank (uspto)